AMENDED IN ASSEMBLY JUNE 23, 2016

AMENDED IN ASSEMBLY JUNE 14, 2016

AMENDED IN SENATE MARCH 29, 2016

SENATE BILL No. 1121

Introduced by Senator Leno

February 17, 2016

An act to amend Sections 1546, ~~1564.1,~~ *1546.1,* and 1546.2 of the Penal Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 1121, as amended, Leno. Privacy: electronic communications: search warrant.

Existing law prohibits a government entity from compelling the production of or access to electronic communication information or electronic device information, as defined, without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, except for emergency situations, as defined. Existing law also specifies the conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, or consent of the owner of the device.

This bill would additionally authorize a government entity, without a warrant or other order, to access electronic device information by means of physical interaction or electronic communication with the device for the purpose of accessing information concerning the location of the electronic device in order to respond to an emergency 911 ~~call.~~ *call from that device.* The bill would also provide that the definition of

"electronic device" for purposes of the bill does not include a magnetic strip on a driver's license or identification card, as prescribed.

Existing law authorizes a service provider to voluntarily disclose electronic communication information or subscriber information. Existing law requires a government entity to destroy that information within 90 days unless one or more specified circumstances apply, including, among others, the government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

This bill would also authorize a government entity to retain the information beyond 90 days if the service provider or subscriber is, or discloses to, a federal, state, or local prison, jail, or juvenile detention facility, and all parties to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1546 of the Penal Code is amended to read:

1546. For purposes of this chapter, the following definitions apply:

(a) An "adverse result" means any of the following:

(1) Danger to the life or physical safety of an individual.

(2) Flight from prosecution.

(3) Destruction of or tampering with evidence.

(4) Intimidation of potential witnesses.

(5) Serious jeopardy to an investigation or undue delay of a trial.

(b) "Authorized possessor" means the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(c) "Electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

(d) "Electronic communication information" means any information about an electronic communication or the use of an

electronic communication service, including, but not limited to, the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. Electronic communication information does not include subscriber information as defined in this chapter.

(e) "Electronic communication service" means a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

(f) "Electronic device" means a device that stores, generates, or transmits information in electronic form. An electronic device does not include the magnetic strip on a driver's license or an identification card issued by this state or a driver's license or equivalent identification card issued by another state.

(g) "Electronic device information" means any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

(h) "Electronic information" means electronic communication information or electronic device information.

(i) "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

(j) "Service provider" means a person or entity offering an electronic communication service.

(k) "Specific consent" means consent provided directly to the government entity seeking information, including, but not limited to, when the government entity is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is a government entity.

(*l*) "Subscriber information" means the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the provider to establish or maintain an account or communication channel, a subscriber or account

number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

SEC. 2. Section 1546.1 of the Penal Code is amended to read:

1546.1. (a) Except as provided in this section, a government entity shall not do any of the following:

(1) Compel the production of or access to electronic communication information from a service provider.

(2) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

(3) Access electronic device information by means of physical interaction or electronic communication with the electronic device. This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity.

(b) A government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) Pursuant to an order for electronic reader records issued pursuant to Section 1798.90 of the Civil Code.

(4) Pursuant to a subpoena issued pursuant to existing state law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law. Nothing in this paragraph shall be construed to expand any authority under state law to compel the production of or access to electronic information.

(c) A government entity may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

(1) Pursuant to a warrant issued pursuant to Chapter 3 (commencing with Section 1523) and subject to subdivision (d).

(2) Pursuant to a wiretap order issued pursuant to Chapter 1.4 (commencing with Section 629.50) of Title 15 of Part 1.

(3) With the specific consent of the authorized possessor of the device.

(4) With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

(5) If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information.

(6) If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the government entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

(7) Except where prohibited by state or federal law, if the device is seized from an inmate's possession or found in an area of a correctional facility or a secure area of a local detention facility where inmates have access, the device is not in the possession of an individual, and the device is not known or believed to be the possession of an authorized visitor. Nothing in this paragraph shall be construed to supersede or override Section 4576.

(8) If the government entity accesses information concerning the location or the telephone number of the electronic device in order to respond to an emergency 911 ~~call.~~ *call from that device.*

(d) Any warrant for electronic information shall comply with the following:

(1) The warrant shall describe with particularity the information to be seized by specifying, as appropriate and reasonable, the time periods covered, the target individuals or accounts, the applications or services covered, and the types of information sought, provided, however, that in the case of a warrant described in paragraph (1) of subdivision (c), the court may determine that it is not appropriate to specify time periods because of the specific circumstances of the investigation, including, but not limited to, the nature of the device to be searched.

(2) The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use, or disclosure except pursuant to a court order or to comply with discovery as required by Sections 1054.1 and

1054.7. A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law.

(3) The warrant shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. If directed to a service provider, the warrant shall be accompanied by an order requiring the service provider to verify the authenticity of electronic information that it produces by providing an affidavit that complies with the requirements set forth in Section 1561 of the Evidence Code. Admission of that information into evidence shall be subject to Section 1562 of the Evidence Code.

(e) When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, do either or both of the following:

(1) Appoint a special master, as described in subdivision (d) of Section 1524, charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.

(2) Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after the termination of the current investigation and any related investigations or proceedings.

(f) A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

(g) If a government entity receives electronic communication information voluntarily provided pursuant to subdivision (f), it shall destroy that information within 90 days unless one or more of the following circumstances apply:

(1) The government entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

(2) The government entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary

disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

(3) The government entity reasonably believes that the information relates to child pornography and the information is retained as part of a multiagency database used in the investigation of child pornography and related crimes.

(4) The service provider or subscriber is, or discloses the information to, a federal, state, or local prison, jail, or juvenile detention facility, and all participants to the electronic communication were informed, prior to the communication, that the service provider may disclose the information to the government entity.

(h) If a government entity obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the government entity shall, within three court days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under paragraph (1) of subdivision (b) of Section 1546.2. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to subdivision (a) of Section 1546.2 if that notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground. This subdivision does not apply if the government entity obtains information concerning the location of the electronic device in order to respond to an emergency 911 ~~call.~~ *call from that device.*

(i) This section does not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

(1) Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

(2) Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

(3) Require a service provider to provide subscriber information.

(j) Nothing in this chapter shall be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity's possession.

SEC. 3. Section 1546.2 of the Penal Code is amended to read:

1546.2. (a) Except as otherwise provided in this section, any government entity that executes a warrant, or obtains electronic information in an emergency pursuant to Section 1546.1, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three court days after obtaining the electronic information.

(b) (1) When a warrant is sought or electronic information is obtained in an emergency under Section 1546.1, the government entity may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

(2) The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in paragraph (1).

(3) Upon expiration of the period of delay of the notification, the government entity shall serve upon, or deliver to by registered

or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant, a document that includes the information described in subdivision (a), a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

(c) If there is no identified target of a warrant or emergency request at the time of its issuance, the government entity shall submit to the Department of Justice within three days of the execution of the warrant or issuance of the request all of the information required in subdivision (a). If an order delaying notice is obtained pursuant to subdivision (b), the government entity shall submit to the department upon the expiration of the period of delay of the notification all of the information required in paragraph (3) of subdivision (b). The department shall publish all those reports on its Internet Web site within 90 days of receipt. The department may redact names or other personal identifying information from the reports.

(d) Except as otherwise provided in this section, nothing in this chapter shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

O